V2X Communication Security, Cyber Security, and Privacy

Dominic Paulraj, Nazeer Shaik, and André Weimerskirch
Lear Corporation
{DPaulraj, NShaik, AWeimerskirch}@lear.com

ABSTRACT

The US Department of Transportation (USDOT) published a notice of proposed rulemaking (NPRM) for vehicle-to-vehicle (V2V) safety communication applications in December 2016, and plans to move forward with the mandatory introduction of V2V in the United States. Security and privacy is a major challenge for V2V deployment though. This paper will provide an overview of the security and privacy challenges, and point towards solutions.

INTRODUCTION

The US Department of Transportation (USDOT) is moving forward with a mandatory vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) safety communications systems to drastically reduce the number of fatalities and accidents. V2V is a wireless 360-degree communication system that allows vehicle safety applications to issue driver warnings such as forward collision warnings, emergency brake warning, etc., when the other vehicle is not in line-of-sight. V2V is based on vehicles' broadcast of Basic Safety Messages (BSM) that include the vehicle's position, velocity, acceleration, current time, and some additional information. BSMs are envisioned to be broadcast 10 times per second. Each receiver is then enabled to predict collisions and warn the driver. The USDOT released a notice of proposed rulemaking (NPRM) in December 2016 that outlines the anticipated technology and policies [DOT16], and Cadillac is about to release the 2017 CTS that will be offered with V2V technology.

Security and privacy are major challenges for a successful deployment of V2V. Security and privacy can be considered on three levels:

1. V2X communication security and user privacy
2. Server security
3. Vehicle cybersecurity

V2X COMMUNICATION SECURITY AND USER PRIVACY

Communication security enables a receiver of a BSM to validate that the BSM was sent by a trustworthy and legitimate device, and that the message was not modified between sender and receiver. Trust is introduced into the system by digitally signing BSMs, and all receivers of the BSM are enabled to digitally verify and validate the message. This requires the use of a public-key infrastructure, which is called Security Credential Management System (SCMS) in the V2V context. The SCMS acts as trust anchor of the security system and provides digital credentials to all vehicles.

The V2X system has been designed with privacy as first priority after safety. In order to protect users' privacy, each vehicle receives a large number of certificates and then rotates over these certificates. For instance, when a vehicle starts driving, it might digitally sign BSMs with Certificate #1, but after 5 minutes it switches to Certificate #2, and so on. This avoids that an

adversary can easily link certificates and track a vehicle. It is currently envisioned that each vehicle receives at least 20 certificates per week to rotate over, however, we feel that a number around 50 certificates per week provides a proper level of privacy. Note that certificates and BSMs do not include any identifying information, or any information that would allow a 3rd party to link certificates. In order to remove misbehaving devices, e.g. devices that broadcast false position information, be it due to a defect or intentional misbehavior, the SCMS supports an efficient revocation scheme. The revocation scheme allows to warn all participants about the misbehaving device and to eventually remove the misbehaving device from the system without revealing the device's identity. Vehicles will check received messages for misbehavior, and ideally also check plausibility of own sensor information to detect sensor defects and forged sensor. For instance, such a plausibility check can detect sudden jumps of GPS location, time, or velocity and acceleration that violate physical laws. If received messages indicate any kind of misbehavior, then the received message is discarded and a report about the detected misbehavior is send to the SCMS. If the plausibility checks of own sensor data fails, the V2X transmitter is turned-off. The complete SCMS design is described in [WWKH13]. The design of the SCMS also protects users' privacy against inside attackers, where an insider (e.g. a hacker or a rogue employee) cannot learn anything about a particular vehicle or its movement pattern.

The security system has also been designed with performance in mind. Since cryptographic operations are expensive, the resource saving verify-on-demand mechanism has been introduced [KW11]. A receiver of a BSM then only verifies a BSM if that BSM would generate a driver warning, otherwise no BSM verification is necessary. For instance, a BSM originates from a vehicle that is 300m away, it will not be relevant for a receiver, and hence there is no need to verify that BSM. Figure 1 provides an overview of the described ideas.

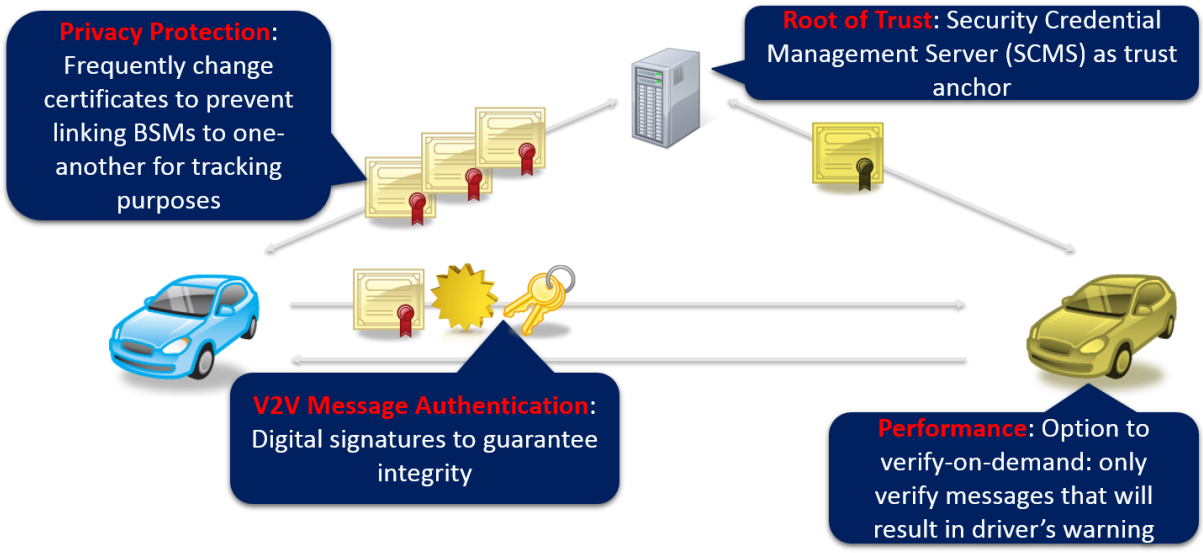

Figure 1: V2V Communication Security

We want to emphasize that the envisioned mandate is for driver warnings only but not for automation features. Hence the main concern are false warnings due to adversaries, which would render the system useless if there are too many false warnings.

The US DOT currently supports several Connected Vehicle Pilot Programs as well as a Smart City program. More information is available in [DOT17] and [DOT17a]. Lear Corporation was selected to provide the on-board units (OBU) and road-side units (RSU) for the Wyoming pilot program, due to Lear's superior V2X solution and extensive expertise in V2X over the last decade [L17]. Note that all pilot programs will connect to an operational SCMS which has been developed by the Crash Avoidance Metrics Partners LLC (CAMP) under a Cooperative Agreement with the US DOT. More information is available in [C16].

SERVER SECURITY

The SCMS has been designed in a flexible manner to support distributed SCMS component instances, e.g., to allow car makers to run some of the components and use some centralized components. It is important to protect all SCMS components against hacker attacks, as is the case for all server systems that are connected to the Internet. Server and Internet security has been widely researched for several decades. Since server security is not specific to the V2X system, we do not further consider the topic here. Note that vehicles must be designed and implemented in a way that a compromised server cannot have any critical impact.

CYBERSECURITY

Several research teams have demonstrated impressively during the last years that it is possible to compromise automotive systems [KCR+10, CMK+11, MV14, MV15]. Attacks have been shown on almost every available interface, such as the diagnostics port, USB, CD/DVD, Bluetooth, and cellular connections. Lear protects all interfaces carefully, and we include the V2X interface in our comprehensive cybersecurity strategy. As such we apply a comprehensive set of security techniques to the V2X interface. We want to point out though that the V2V input will eventually be used as an additional sensor beyond camera, radar, and/or lidar for automated functions such as brake assist. Hence additional cybersecurity considerations for the V2V wireless interface are necessary.

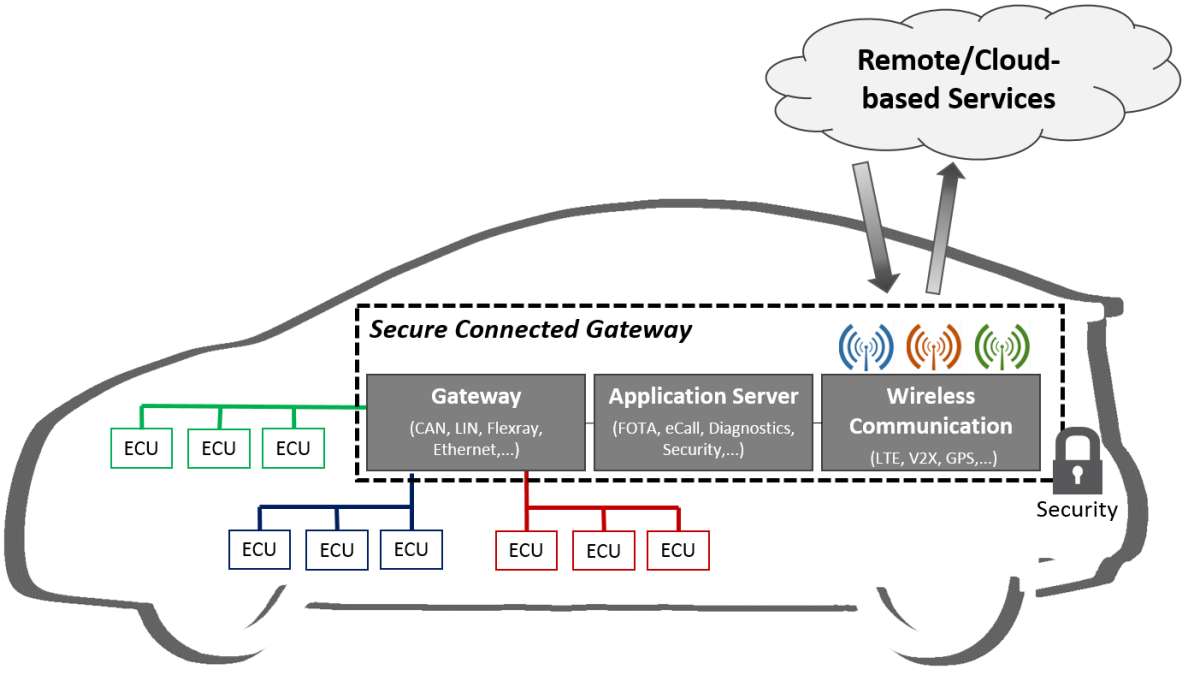

Figure 2: Lear's Connected Gateway

Figure 2 display's Lear's Connected Gateway which is V2X capable. Lear's connected gateway uses a secure architecture that separates external communication interfaces to internal safety systems, such as powertrain and ADAS, via physical (wireless communication and real-time safety critical applications run on separate microcontrollers) and/or logical separation (software separation, hypervisor, and/or software containers). Further security features include secure micro-controllers and secure boot, secure software over-the-air (SOTA), hardened kernel, dynamic firewall for all interfaces, secure communication, deactivated debug interfaces, and secure key storage. Note that Lear applies a secure cybersecurity engineering process to apply proper security mechanisms for each product. Figure 3 summarizes Lear's cybersecurity platform.

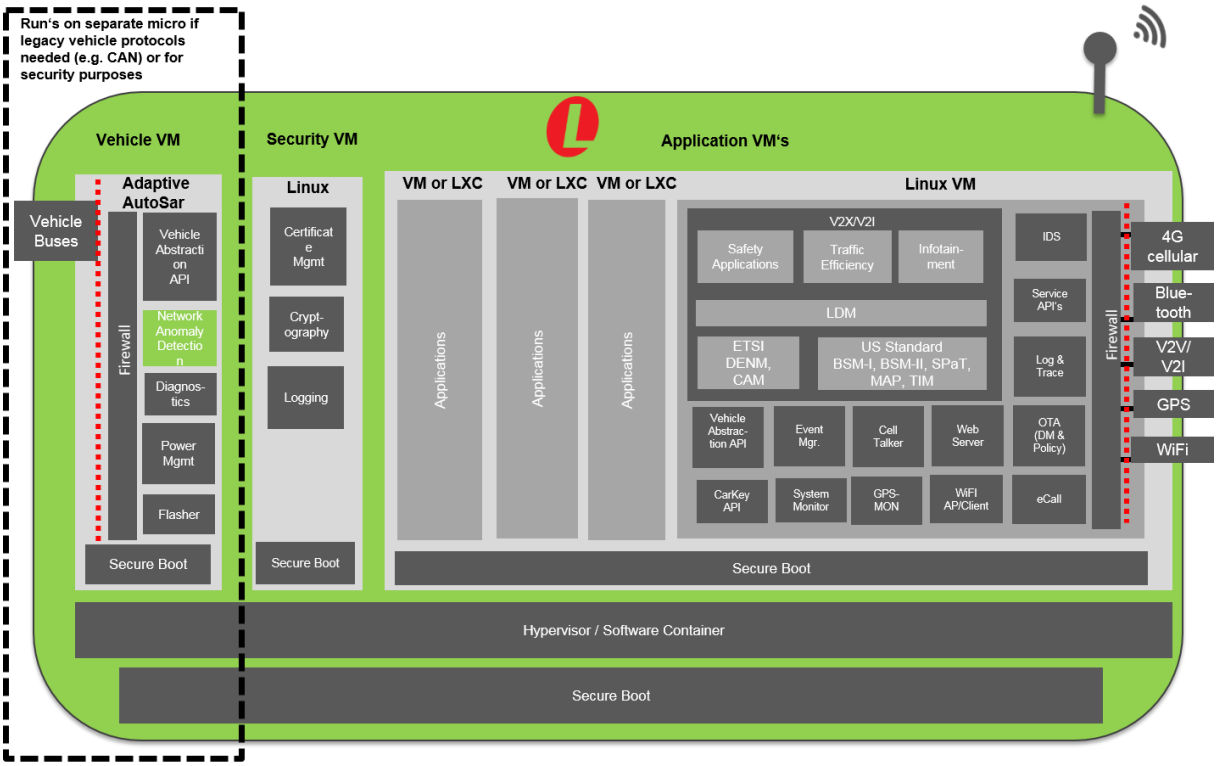

Figure 3: Lear's Secure Reference Platform

Proper cybersecurity mechanisms are required to avoid direct attacks to the vehicle's behavior in the first place. However, an attacker might still extract keys from a vehicle with great effort and then forge or manipulate BSMs that are broadcast over the air in order to provide false information. It is necessary to closely combine the safety and security consideration of V2V systems, especially once V2V systems are used as an additional sensor to camera, radar and/or lidar for automation features. For instance, strategies need to be developed if the V2V sensor and a camera sensor provide contradicting information, which might be because there is no line-of-sight available, or due to an adversary. A starting point is to use confidence levels for the sensor input, where camera likely has the highest confidence level, V2V has the lowest confidence level, and radar and lidar have a confidence level in between.

CONCLUSIONS

The US DOT moves forward to introduce V2V communication safety applications in all new vehicles. Security and privacy is a main challenge towards deployment of V2V. This article provides an overview of the different aspects around security and privacy, and considers communication security, server security, cybersecurity, and privacy. While server security is well understood, there are still open issues around privacy and V2V application design. For instance, it is important to understand how many certificates per week each device should hold for a sufficient level of privacy. Once V2V is connected to automation systems as an additional sensor to camera, radar, and/or lidar, it is essential to combine cybersecurity and safety considerations for the design of such V2V applications.

REFERENCES

[CMK+11] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, *Comprehensive Experimental Analyses of Automotive Attack Surfaces,* USENIX Security Symposium, 2011.

[C16] Crash Avoidance Metrics Partners (CAMP) LLC, *Security Credential Management System Proof-of-Concept Implementation – EE Requirements and Specifications Supporting SCMS Software Release 1.1*, 2016, available at https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf.

[KCR+10] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, *Experimental security analysis of a modern automobile*, 2010 IEEE Symposium on Security and Privacy, 2010.

[KW11] Hariharan Krishnan and André Weimerskirch, *Verify-on-Demand - A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication*, SAE 2011 World Congress, 2011.

[L17] Lear Corporation, *Lear Corporation Selected by Wyoming Department of Transportation for Connected Vehicle Pilot Program*, 2017, available at http://www.lear.com/Press-Room/4414/lear-corporation-selected-by-wyoming-department-of-transportation-for-connected-v.aspx

[MV14] Charlie Miller and Chris Valasek, *Adventures in Automotive Networks and Control Units*, 2014, available at https://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf.

[MV15] Charlie Miller and Chris Valasek, *Remote Exploitation of an Unaltered Passenger Vehicle*, 2015, available at http://illmatics.com/Remote%20Car%20Hacking.pdf

[DOT16] United State Department of Transportation – National Highway Traffic Safety Administration, *U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashes*, 2016, available at https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands

[DOT17] United State Department of Transportation, - Intelligent Transportation Systems - Joint Program Office, *Connected Vehicle Pilot Deployment Program*, available at http://www.its.dot.gov/pilots/index.htm.

[DOT17a] United States Department of Transportation, *Smart City Challenge*, available at https://www.transportation.gov/smartcity.

[WWKH13] William Whyte, André Weimerskirch, Virendra Kumar, and Thorsten Hehn, *A Security Credential Management System for V2V Communications*, 2013 IEEE Vehicular Networking Conference (VNC 2013), 2013.